Detección de Anomalías en Oráculos Criptográficos tipo RSA por medio de análisis probabilísticas y estadísticos.

Ing. Antonio CASTRO LECHTALER[1] Msc.
Lic. Marcelo Cipriano[2]

Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Escuela Superior Técnica "Gral Div. Manuel N. Savio".
Facultad de Ingeniería.
Instituto de Educación Superior del Ejército Argentino.

[1]acastro@iese.edu.ar
[2]marcelocipriano@iese.edu.ar

1.Resumen.

Esta línea de investigación persigue la elaboración de herramientas matemáticas susceptibles de ser sistematizadas en un software que sea capaz de detectar anomalías y mal funcionamiento en servicios de autenticación de usuarios o equipos, claves de sesión y cualquier otro servicio criptográfico que utilice el esquema RSA. Para aplicar en redes Públicas o Privados, Lan´s, o Wan´s o asimismo Internet. En entornos de aplicación dual, es decir tanto en sistemas militares como del ámbito civil.

Dada la complejidad de los sistemas actuales, se hace cada vez más complicada la detección de determinado tipos de errores los cuales, al no ser depurados, pasan de las versiones de pruebas a las versiones a ejecutar en los sistemas y redes.

Promediando ya la línea investigativa y ya superadas las etapas de planteamiento del problema, investigación, análisis y desarrollo de las herramientas matemáticas, se procede a iniciar la etapa de codificación de las herramientas.

Luego se deberán realizar las pruebas de eficacia y eficiencia del software desarrollado para luego, en caso de satisfacer todos los requerimientos, finalizar con la implementación de la solución desarrollada.

2. Palabras Claves.

Seguridad en Redes, Detección de Anomalías, Open-SSL, RSA.

3. Contexto.

El Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática pertenece a la Escuela Superior Técnica –Facultad de Ingeniería- del Ejército Argentino en el área del Posgrado en Criptografía y Seguridad Informática que se dicta en esta institución, junto a otros posgrados y carreras de grado en ingeniería.

El desarrollo científico y tecnológico es relevante a nivel estratégico y es por ello que tanto las Fuerzas Armadas en general como el Ejército en particular.

El Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF) realizó aportes a través de Proyectos de Investigación Científico Tecnológicos Orientados (PICTO) para la realización durante 6 años del proyecto recientemente finalizado sobre "REDES PRIVADAS COMUNITARIAS", -dentro del cual se llevó adelante gran parte de esta investigación-, cuyos resultados parciales o finales han sido presentados en varios CACIC para su difusión a la comunidad científica.

4. Introducción.

4.1. Generalidades

Desde que la Criptografía dejó de pertenecer a la esfera de los secretos militares y diplomáticos, para volcarse al ámbito civil -luego de la explosión informática de los años `80 y `90 no han dejado de crecer sus aplicaciones. Desde la consulta de mails, ingreso a redes sociales, home banking o compras online, son requeridos sus servicios para proteger la información de los usuarios y sistemas.
La conexión de los usuarios y sus equipos a diversas redes, desde las hogareñas hasta las públicas, requiere de servicios de autenticación y cifrado de datos.

Todo lo que implique intercambio de información entre dos equipos informáticos debería estar al resguardo de técnicas criptográficas. Pero esto al usuario le resulta transparente. Los sistemas se encargan de entablar todos los servicios requeridos por los estándares y protocolos de manera automática
Tickets de ingreso a sistemas, intercambios de claves, autenticación de usuarios y equipos, inicio de sesión, y muchos otros servicios son controlados en forma automática, a menos que el usuario tome el control y cambie las opciones por defecto.

¿Cómo comprobar si estos procesos y servicios contienen errores que pueden alterar la seguridad de lo que pretenden proteger?
Llamaremos Oráculo a un servicio que ofrezca a sus clientes claves públicas, privadas y módulos en un esquema de cifrado/descifrado RSA[1].

4.2. Código abierto no necesaria-mente aumenta la Seguridad de los Sistemas de Información.

En la industria del software conviven dos modalidades para el desarrollo de software: abiertos y cerrados. La diferencia, básicamente radica en la posibilidad que los usuarios puedan o no ver los códigos fuentes de los mismos.
La solución de software abierto (open source) Seguridad de los Sistemas de Información, es mucho más atractiva que la de software cerrado dado que se puede "ver" lo que el sistema hace y cómo lo hace. La ausencia de "puertas traseras" o claves no documentadas u otras técnicas como la inoculación de código virulento [01]. Aunque estén abiertos sus códigos no significa que se encuentren libres de errores.

No todos los usuarios pueden leer el código e interpretar su significado y de esa manera corroborar el correcto funcionamiento del servicio. Luciano Bello ha descubierto un error en

[1] La 3-tupla (n,e,d): n (módulo) es el producto de 2 primos, e (clave pública) y d (clave privada) son inversos entre sí mód $\phi(n)$.

OpenSSL[2]. Que fue enmendado 20 meses después que la versión defectuosa. [02].

Según la Ley de Linus "dado un número muy grande de ojos, los errores se convierten en evidentes" [03].

Está claro que al tiempo que aumenta la sofisticación y complejidad de los códigos, la cantidad de ojos disponibles para evidenciar los errores decrece. Es por ello que automatizar el análisis del funcionamiento del software en busca de anomalías se hace cada vez más necesario.

4.3. Planteamiento del problema.

Un oráculo tipo Open-SSL que ofreciera protección criptográfica (en sus diferentes formas antes mencionadas: claves de sesión, autenticación de equipos, etc.) es vulnerable cuando:

1) Oráculo genera un número relativamente pequeño de primos[3].

2) Oráculo está diseñado con una directiva errónea para la selección de los primos o la generación de los módulos.

En ambos casos Oráculo se distancia del comportamiento equiprobable, dentro de ciertos parámetros asumidos, a un comportamiento sesgado. Susceptible de ser estudiado por un atacante y vulnerar así el sistema.

3) Un atacante tiene forma de construir *un subconjunto P´de Primos con los que trabaja* tal que el conocimiento de P´ le permita vulnerar la factorización de RSA para una cantidad significativa de módulos.

Vemos que se deben hallar los factores primos del esquema RSA, proceso complejo pues esa es la fortaleza que permite a esta criptosistema proteger la información: la complejidad en la factorización de un número enorme.

5. Resultados y Objetivos.

5.1. Resultados intermedios de la línea de Investigación.

En el año 2008 nuestra investigación se oriento a la elaboración una herramienta informática que permite hallar los primos que componen un módulo RSA con la información que aportan su clave pública y su clave privada, resultado presentado y publicado en CACIC 2008 [04] realizado en La Rioja, Argentina.

Las posteriores pruebas de codificación e implementación demostraron que este procedimiento corría muy veloz presentándose estos resultados en CUBA [05].

Seguimos aún estudiando el comportamiento de este algoritmo y lo comparamos con el procedimiento que aborda el mismo problema y lo resuelve, existente en la bibliografía tradicional para la enseñanza de la criptografía [06].

Los análisis indicaron que la complejidad computacional de nuestro algoritmo era del orden O (log n) mientras que el de la bibliografía de referencia tenía un orden O ($\log^3$ n). Resultado presentado en Santiago de Chile y que nos sorprendió de manera grata [07].

[2] Una mala inicialización de una variable provocó una predictibilidad en el generador de números, abriendo una vulnerabilidad inimaginable.

[3] Vulnerabilidad de OpenSSL de Devian descubierta por L. Bello.

Con las herramientas de análisis en nuestras manos, eficaces y altamente eficientes, abordamos el estudio de la detección de anomalías por medio de la búsqueda de colisiones entre los primos de un generador de módulos criptográficos de tipo RSA en un sistema oráculo de tipo Open SSL.

Hallada la herramienta matemática que permitiría detectar anomalías (en caso que las hubiere) el resultado publicado en CACIC 2011 [08] realizado en la Facultad de Informática de La Plata el pasado año.

5.2. Etapa actual

Se ensamblaron y codificaron todas las herramientas matemáticas antes mencionadas, en una plataforma de software programado en C++. Tarea realizada por el Teniente Primero Eduardo MALVACIO, estudiante de Ingeniería Informática de nuestra facultad, en la cátedra de Computación I a cargo del Ing. Mg. Alejandro Repetto.

Pronto finalizará la etapa de programación, las pruebas de implementación y depurado de errores.

5.3. Etapa final.

Hemos diseñado un experimento para evaluar este algoritmo:

Manipularemos a oráculo para que presente vulnerabilidades. Y pondremos a correr el programa. De manera aleatoria repetiremos el experimento con oráculos vulnerables como así también sin manipular.

Se espera que el programa sea capaz de detectar los oráculos vulnerables y alertar acerca de ellos. Asimismo informar también sobre los oráculos seguros.

El experimento se repetirá gran cantidad de veces, registrando los falsos positivos como los negativos si los hubiere. De esa forma estudiar la eficacia y eficiencia de esta herramienta.

Cabe aclarar que dada la magnitud en tamaño y la enorme cantidad de valores con las que trabajan estos oráculos, el abordaje es probabilístico-estadístico.

Publicaremos estos resultados en los próximos meses. Es nuestra intención poder hacerlo en el CACIC 2012.

6. Formación de Recursos Humanos.

Algunos algoritmos fueron codificados y probados en el contexto de la Cátedra de Computación I a cargo del Ing. Mg. Alejandro Repetto, que posee nuestra facultad en la carrera de Ingeniería Informática,

Si bien aún el laboratorio no posee ningún becario doctorando o post-doctorando, el resto de los integrantes del equipo son investigadores categorizados en el programa de Incentivos del Ministerio de Ciencia, Tecnología e Innovación Productiva y en el Sistema Científico Tecnológico de la Defensa en el régimen de Régimen para el personal de Investigación y Desarrollo de las Fuerzas Armadas (RPIDFA).

7. Referencias y Bibliografía

[01] Young A and Yung M. An Elliptic Curve Asymmetric Backdoor in OpenSSL RSA Key Generation. Chapter 10. Cryptovirology. 2006. http://www.cryptovirology.com.

[02] Bello L, Bertacchini M. "*Generador de Números Pseudo-Aleatorios Predecible en Debian"*. III Encuentro Internacional de Seguridad Informática. Manizales, Colombia. Octubre 2009.

[03] Glass, Robert "*Facts and Fallacies of Software Engineering"*. Addison-Wesley Professional, 2003.

[04] Cipriano, M. "*Factorización de N: recuperación de factores primos a partir de las claves pública y privada*." Anales del XIV Congreso Argentino de Ciencias de la Computación CACIC 2008. Chilecito, La Rioja, Octubre 2008.

[05] Castro Lechtaler, C; Cipriano, M; Benaben A; Quiroga, P. "*Study on the effectiveness and efficiency of an algorithm to factorize N given e and d"* Anales del IX Seminario Iberoamericano en Seguridad de las Tecnologías de la Información, La Habana, CUBA. 2009.

[06] Menezes, A; van Oorschot, P and Vanstone, S. *Handbook of Applied Cryptography*. CRC Press. 5th Edition, 2001.

[07] Benaben, A; Castro Lechtaler, A; Cipriano, M; Foti, A. "*Development, testing and performance evaluation of factoring algorithms whit additional information*" XXVIII Conferencia Internacional de la Sociedad Chilena de Computación. Santiago de Chile

[08] Castro Lechtaler, A; Cipriano, M. "*Detección de anomalías en Oráculos tipo OpenSSL por medio del análisis de probabilidades*" Anales del XVII Congreso Argentino de Ciencias de la Computación CACIC 2011. La Plata, Buenos Aires, Octubre 2011.